

REMARKS/ARGUMENTS

1.) Claim Amendments

Claims 4, 8-14, 16-19, 22, 31-37, 39-41, 51, and 52 are pending in the application. The Applicants have amended claims 51 and 52. Favorable reconsideration of the application is respectfully requested in view of the foregoing amendments and the following remarks.

2.) Examiner Objections

The Examiner objected to the specification for failing to provide proper antecedent basis for the claimed subject matter, namely the following limitations recited in claim 51:

encrypting authentication and authorization information in a mobile node;
sending the encrypted authentication and authorization information;
forwarding the encrypted authentication and authorization information; and
performing an analysis of the encrypted authentication and authorization information. (emphasis added by the Examiner).

Thus the Examiner contends the specification does not support the claim that in the initial exchange between the mobile node and the network, the authentication and authorization information is encrypted. In past responses, the Applicants have referred to the statement in the specification on page 7, lines 17-21 for supporting this limitation. The specification states, "It will also be possible to apply prior encryption between MN and AAAh (e.g. EAP/TLS [4]) since the exchanges are not visible over the air interface. This means that satisfactory security against eavesdropping, man-in-the-middle and other attacks can be maintained for mobile nodes roaming in foreign networks." The Examiner contends this disclosure is inadequate.

Further support for this limitation is found in Reference [4] "EAP Tunneled TLS Authentication Protocol", Paul Funk, Simon Blake-Wilson, November 2002, listed on page 34 of the specification, and referred to in the statement on page 7, lines 17-21. Reference [4] can be found at <http://tools.ietf.org/html/draft-ietf-pppext-eap-ttls-02>. The

architecture model picture described in Section 4 illustrates a secure password authentication tunnel from the client (i.e., MN) to a TTLS AAA Server. As described in Section 4.1:

The keying material used to encrypt and authenticate the data connection between the client and access point is developed implicitly between the client and TTLS server as a result of EAP-TTLS negotiation. This keying material must be communicated to the access point by the TTLS server using the AAA carrier protocol.

The client and access point must also agree on an encryption/validation algorithm to be used based on the keying material. In some systems, both these devices may be preconfigured with this information, and distribution of the keying material alone is sufficient. Or, the link layer protocol may provide a mechanism for client and access point to negotiate an algorithm.

Thus, the MN and AAA server may be preconfigured with keying material so that the initial messages can be encrypted. EAP-TTLS can be applied to various authentication protocols as described in Section 10.2. EAP is also described in Section 10.2.1. Thus, the EAP-MIPv6 protocol described in the Applicants' specification can also be applied to EAP-TTLS. In this manner, EAP-MIPv6 information is encrypted and sent through the visited network as claimed. Therefore, the withdrawal of the objection is respectfully requested.

3.) Claim Rejections – 35 U.S.C. § 112, first paragraph

The Examiner rejected claims 4, 8-14, 16-19, 22, 31-37, 39-41, and 51-52 under 35 U.S.C. § 112, first paragraph as failing to comply with the written description requirement due to the alleged lack of support for the encrypting step discussed above. The Applicants respectfully submit that the support is found in Reference [4] as discussed above. Therefore, the withdrawal of the § 112 rejection is respectfully requested.

4.) Claim Rejections – 35 U.S.C. § 102(e)

The Examiner rejected claims 4, 16-17, 19, 39-40 and 51-52 under 35 U.S.C. § 102(e) as being anticipated by Faccin, et al. (US 2002/0120844, hereinafter "Faccin

'844"). The Applicants have amended the claims to better distinguish the claimed invention from Faccin '844. The Examiner's consideration of the amended claims is respectfully requested.

Independent claims 51 and 52 recite that the AAA client in the visited network is a pass-through node. The Examiner argues that the specification does not define this feature. However, support for this feature is found in Reference [16] "Extensible Authentication Protocol (EAP)", L. Blunk, J. Vollbrecht, B. Aboda, J. Carlson, H. Levkowitz, September 2003, listed on page 35 of the specification. Reference [16] can be found at <http://tools.ietf.org/html/draft-ietf-eap-rfc2284bis-06>. Section 2.3 defines pass-through behavior as follows:

Where an authenticator operates as a pass-through, it forwards packets back and forth between the peer and a backend authentication server, based on the EAP layer header fields (Code, Identifier, Length). This includes performing validity checks on the Code, Identifier and Length fields, as described in Section 4.1.

Since pass-through authenticators rely on a backend authenticator server to implement methods, the EAP method layer header fields (Type, Type-Data) are not examined as part of the forwarding decision. The forwarding model is illustrated in Figure 2. Compliant pass-through authenticator implementations MUST by default be capable of forwarding packets from any EAP method. The use of the RADIUS protocol for encapsulation of EAP in pass-through operation is described in [RFC3579].

The Applicants respectfully submit that the nodes in the Visited Domain in Faccin '844 do not act as mere pass-through nodes. In paragraph 0065, Faccin '844 states, "Before transmitting it to the home domain, the visited domain adds its own DH value encrypted with K1, i.e. the security association shared between the visited domain 202 and the home domain 204." In paragraph 0068, Faccin '844 also states that the visited domain adds DH information to messages going to the MN as well. Adding information to the messages is not acting as a pass-through node.

Thus, Faccin '844 does not teach or suggest all of the claimed limitations of independent claims 51 and 52. Therefore, the allowance of amended claims 51 and 52 is respectfully requested.

Claims 4, 16, 17, 19, 39, and 40 depend from amended claims 51 or 52 and recite further limitations in combination with the novel elements of claims 51 or 52. Therefore, the allowance of amended claims 4, 16, 17, 19, 39, and 40 is respectfully requested.

5.) Claim Rejections – 35 U.S.C. § 103(a)

The Examiner rejected claims 8-10, 12-14, 22, 31-33 and 35-37 under 35 U.S.C. § 103(a) as being unpatentable over Faccin '844 , as applied to claims 51 and 52 above, in view of Faccin et al., (hereinafter "Faccin_Internet-Draft), "Diameter Mobile IPv6 Applicationn draft-le-aaa-diameter-mobileip6-6-03.txt", Internet Draft, XP015004098, published in April 2003.

The Applicants respectfully submit that the amendments made to independent claims 51 and 52 to overcome the novelty rejection above also distinguish the claimed invention from the combination of Faccin '844 and Faccin_Internet-Draft. Faccin_Internet-Draft also fails to disclose or suggest sending encrypted authentication and authorization information through pass-through nodes in the visited network. Claims 8-10, 12-14, 22, 31-33 and 35-37 depend from amended claims 51 or 52 and recite further limitations in combination with the novel and unobvious elements of claims 51 or 52. Therefore, the allowance of claims 8-10, 12-14, 22, 31-33 and 35-37 is respectfully requested.

The Examiner rejected claims 11 and 34 under 35 U.S.C. § 103(a) as being unpatentable over Faccin '844 and Faccin_Internet-Draft, as applied to claims 51 and 52 above, and further in view of Akhtar, et al. (US 7,079,499).

The Applicants respectfully submit that the amendments made to independent claims 51 and 52 to overcome the novelty rejection above also distinguish the claimed invention from the combination of Faccin '844, Faccin_Internet-Draft, and Akhtar. The Examiner cites Akhtar for showing EAP TLV attributes. However, Akhtar also fails to disclose or suggest combining a protocol such as EAP with MIPv6 as claimed by the Applicants. Thus, the combination of Faccin '844, Faccin_Internet-Draft, and Akhtar does not teach or suggest sending encrypted authentication and authorization

information through pass-through nodes in the visited network. Claims 11 and 34 depend from amended claims 51 or 52 and recite further limitations in combination with the novel and unobvious elements of claims 51 or 52. Therefore, the allowance of claims 11 and 34 is respectfully requested.

The Examiner rejected claims 18 and 41 under 35 U.S.C. § 103(a) as being unpatentable over Faccin '844, as applied to claims 51 and 52 above, in view of Akhtar, et al. (US 7,079,499).

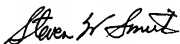
The Applicants respectfully submit that the amendments made to independent claims 51 and 52 to overcome the novelty rejection above also distinguish the claimed invention from the combination of Faccin '844 and Akhtar. As noted above, Akhtar fails to disclose or suggest combining a protocol such as EAP with MIPv6 as claimed by the Applicants. Thus, the combination of Faccin '844 and Akhtar does not teach or suggest sending encrypted authentication and authorization information through pass-through nodes in the visited network. Claims 18 and 41 depend from amended claims 51 or 52 and recite further limitations in combination with the novel and unobvious elements of claims 51 or 52. Therefore, the allowance of claims 18 and 41 is respectfully requested.

6.) Conclusion

In view of the foregoing remarks, the Applicants believe all of the claims currently pending in the Application to be in condition for allowance. The Applicants, therefore, respectfully request that the Examiner withdraw all rejections and issue a Notice of Allowance for claims 4, 8-14, 16-19, 22, 31-37, 39-41, 51, and 52.

The Applicants request a telephonic interview if the Examiner has any questions or requires any additional information that would expedite the prosecution of the Application.

Respectfully submitted,



Steven W. Smith
Registration No. 36,684

Date: June 14, 2010

Ericsson Inc.
6300 Legacy Drive, M/S EVR 1-C-11
Plano, Texas 75024

(972) 583-1572
steve.xl.smith@ericsson.com